

Autorisations uniques de la CNIL de mise en œuvre de dispositifs biométriques

(délibérations nos 2006-101 et 102 du 27 avril 2006, non reproduites, disponibles sur www.cnil.fr)

OBSERVATIONS :

1. Les systèmes biométriques sont “des applications permettant l'identification automatique ou l'éligibilité d'une personne à se voir reconnaître certains droits ou services (notamment l'accès) basés sur la reconnaissance de particularités physiques (empreintes digitales, iris de l'œil, contour de la main, etc.), de traces (ADN, sang, odeurs), ou d'éléments comportementaux (signature, démarche)” (CNIL 22^e rapp. d'activité 2001 p. 157 ; add. 26^e rapp. d'activité 2005 p. 49 ; v. site www.cnil.fr).
2. La CNIL énonce en trois points sa doctrine en la matière :

« 1 - Les technologies de reconnaissance biométrique ne reposant pas sur le stockage des gabarits dans une base de données ne soulèvent pas de difficulté particulière en termes « informatique et libertés », dès lors que le gabarit est conservé sur soi (une carte à puce) ou sur un appareil dont on a l'usage exclusif (un téléphone portable, un ordinateur, etc.) et nulle part ailleurs.

2 - En revanche, lorsqu'une base de données est constituée dans le cadre d'un dispositif d'identification biométrique, l'élément biométrique retenu peut avoir une incidence sur nos libertés et notre vie privée ; tel est le cas lorsque l'élément biométrique retenu « laisse des traces » dans notre vie quotidienne (ADN, empreinte digitale). Dans un tel cas, le contrôle de finalité et de proportionnalité peut conduire à accepter la mise en œuvre de telles bases de données lorsqu'un impératif particulier de sécurité le justifie.

3 - À défaut d'une telle justification particulière, et lorsqu'une base de données de gabarits est constituée, le choix d'un élément biométrique « ne laissant pas de trace », tel que le contour de la main, la rétine, la reconnaissance vocale, etc. devrait être préféré à la prolifération de fichiers d'ADN ou d'empreintes digitales » (rapp. 2001 prec. p. 171). Le rapport 2005 précise encore que la distinction des biométries portant sur des éléments “à traces” ou “sans traces” repose sur la possibilité ou non de récupérer une donnée biométrique à l'insu de la personne.
3. L'article 25 I de la loi 78-17 du 6 janvier 1978 dispose désormais que “Sont mis en œuvre après autorisation de la CNIL (...) 8° les traitements automatisés comportant des données biométriques nécessaires au contrôle de l'identité des personnes”. Toutefois, plutôt qu'un acte autorisant la création du traitement (art. 29), la CNIL peut choisir d'opérer selon une procédure nettement allégée. L'article 25-II précise à cet effet que “les traitements qui répondent à une même finalité, portent sur des catégories de données identiques et ont les mêmes destinataires ou catégories de destinataires peuvent être autorisés par une décision unique de la Commission. Dans ce cas, le responsable de chaque traitement adresse à la commission un engagement de conformité de celui-ci à la description figurant dans l'autorisation”. Par ce mécanisme, la CNIL émet une *autorisation unique* portant sur une forme de traitement et les entreprises ou organismes n'ont alors aucune autorisation à demander mais s'engagent simplement à respecter le cadre général tracé par l'AU.
4. La première autorisation (AU-007) concerne des dispositifs employant une technologie typiquement sans traces (contour de la main) tandis que la seconde use des empreintes digitales mais réserve l'enregistrement de leur gabarit à un support individuel détenu par la personne concernée (AU-008). Sur la base de la doctrine précédemment rappelée, ces particularités garantiraient l'innocuité du dispositif et justifieraient le recours à la procédure d'autorisation unique. On peut pourtant être dubitatif sur ce raisonnement.
5. Il est crucial de s'interroger sur les atteintes aux libertés publiques dont peuvent être porteuses de telles technologies, notamment en matière policière (rapp. 2001 p. 166 s.), et les organisations syndicales sont vigilantes sur cet aspect (M. Jacek, *Le Peuple* n° 1633 du 12 juil. 2006 p. 27 ; C. Labbe “Vers un fichage total ?” *Options* n° 515 du 2 oct. 2006). Mais il serait tout aussi opportun de raisonner en termes de droits fondamentaux afin de déterminer si le contrôle de l'accès aux locaux sur les lieux de travail (AU-008) et la gestion des horaires de travail et la restauration (AU-007) sont des finalités suffisantes, qui ne peuvent être obtenues par des moyens plus proportionnés, pour valider la démarche d'un employeur procédant par le biais d'un système biométrique (A. Cœuret, B. Gauriau, M. Miné, *Droit du travail*, 2006, Sirey, § 555). Qui plus est en empruntant une voie dépourvue de tout examen systématique par l'autorité administrative en charge de ces questions.